

Вариант 7

Зашифрованное сообщение	GAVFVDGDFAVAADADDFAGFA
Ключ	key

Вариант 8

Зашифрованное сообщение	FFDDXAVXFGFA
Ключ	moon

Вариант 9

Зашифрованное сообщение	GDDDDFFXGAFFDF
Ключ	poem

Вариант 10

Зашифрованное сообщение	DFDFAXXFGD
Ключ	note

Шифр Хилла

Шифр Хилла — некий шифр подстановки, который в 1929 году разработал математик Лестер С. Хилл. Данный шифр основывается на линейной алгебре.

Шифрование

Открытый текст представляет собой n -мерный вектор. Ключ – квадратная матрица размера $n \times n$. Для получения шифротекста ключ умножается на открытый текст по модулю выбранной числовой схемы, в случае русского алфавита - 33.

Пусть " $p_1 p_2 p_3$ " – открытый текст, ключ – матрица размера 3×3 и шифротекст – вектор размерности – 3, " $c_1 c_2 c_3$ " соответственно.

В общем виде: $C = K * P$

В матричном виде эта система описывается так:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} * \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}. \quad (4)$$

Или в качестве системы уравнений:

$$\begin{cases} c_1 = k_{11} * p_1 + k_{12} * p_2 + k_{13} * p_3; \\ c_2 = k_{21} * p_1 + k_{22} * p_2 + k_{23} * p_3; \\ c_3 = k_{31} * p_1 + k_{32} * p_2 + k_{33} * p_3. \end{cases} \quad (5)$$

Из уравнений видно, что каждый символ открытого текста участвует в шифровании шифротекста. Именно поэтому шифр Хилла принадлежит к категории блочных шифров.

Пример

В следующем примере используются буквы от А до Я, соответствующие им численные значения приведены в таблице.

Таблица 28. Численное значение букв алфавита

№	Буква	№	Буква	№	Буква
1	А	12	К	23	Х
2	Б	13	Л	24	Ц
3	В	14	М	25	Ч
4	Г	15	Н	26	Ш
5	Д	16	О	27	Щ
6	Е	17	П	28	Ъ
7	Ё	18	Р	29	Ы
8	Ж	19	С	30	Ь
9	З	20	Т	31	Э
10	И	21	У	32	Ю
11	Й	22	Ф	33	Я

Пример

Сообщение: РТУИИИ – 18 20 21 10 10 10

Ключ

$$\begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

Шифрование

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 18 \\ 20 \\ 21 \end{pmatrix} \bmod 33 = \begin{pmatrix} 13 \\ 22 \\ 16 \end{pmatrix} = \begin{pmatrix} Л \\ Ф \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} C4 \\ C5 \\ C6 \end{pmatrix} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 10 \\ 10 \\ 10 \end{pmatrix} \bmod 33 = \begin{pmatrix} 19 \\ 18 \\ 27 \end{pmatrix} = \begin{pmatrix} С \\ Р \\ Щ \end{pmatrix}$$

Зашифрованное сообщение: ЛФОСРЩ

При дешифровании используется следующее правило:

$P = K^{-1} * C$, где K^{-1} – обратная матрица.

Обратная матрица A^{-1} — матрица, произведение которой на исходную матрицу А равно единичной матрице Е. Обратная матрица существует только для квадратных матриц определитель которых не равен нулю.

Дешифрование

$$\begin{pmatrix} P1 \\ P2 \\ P3 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} * \begin{pmatrix} 13 \\ 22 \\ 16 \end{pmatrix} \bmod 33 = \begin{pmatrix} 18 \\ 20 \\ 21 \end{pmatrix} = \begin{pmatrix} Р \\ Т \\ У \end{pmatrix}$$

$$\begin{pmatrix} P4 \\ P5 \\ P6 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} * \begin{pmatrix} 19 \\ 18 \\ 27 \end{pmatrix} \bmod 33 = \begin{pmatrix} 10 \\ 10 \\ 10 \end{pmatrix} = \begin{pmatrix} И \\ И \\ И \end{pmatrix}$$

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Исходное сообщение	КИБ
Ключ	$\begin{matrix} 1 & 3 & 8 \\ 11 & 6 & 16 \\ 9 & 14 & 20 \end{matrix}$

Вариант 2

Исходное сообщение	КТСО
Ключ	$\begin{matrix} 2 & 5 & 10 & 5 \\ 17 & 3 & 15 & 7 \\ 6 & 11 & 26 & 3 \\ 1 & 23 & 9 & 3 \end{matrix}$

Вариант 3

Исходное сообщение	МИРЭА
Ключ	1 3 9 4 1 12 5 14 7 5 3 12 20 5 7 2 26 8 2 4 6 30 29 1 4
Зашифрованное сообщение	ИГХВЕ

Вариант 4

Исходное сообщение	ГРУППА
Ключ	2 5 9 4 3 1 12 5 12 1 2 3 5 12 15 1 4 11 2 23 8 5 6 5 6 26 20 3 4 1 3 13 16 2 1 6

Вариант 5

Исходное сообщение	РТУ
Ключ	2 5 10 12 9 11 6 18 29

Вариант 6

Исходное сообщение	КУРС
Ключ	6 2 9 21 10 2 13 11 8 20 17 4 7 1 12 22

Вариант 7

Исходное сообщение	ПАРА
Ключ	9 21 5 27 6 7 18 11 3 9 24 19 1 18 30 12

Вариант 8

Исходное сообщение	МОРЕ
Ключ	1 18 30 12 3 9 24 19 6 7 18 11 9 21 5 27

Вариант 9

Исходное сообщение	ФАЙЛ
Ключ	2 5 10 5 1 23 9 3 17 3 15 7 6 11 26 3

Вариант 10

Исходное сообщение	УРОК
Ключ	32 1 8 12 6 18 22 9 16 7 4 23 14 10 2 17

Шифр Рамзая

Шифр Рамзая представляет собой шахматный шифр, на который еще накладывается несколько перестановок. В середине 1930-х годов он использовался советскими разведчиками. Одним из самых значимых людей в

истории советского шифрования является Рихард Зорге. Этот шифр, однако, не может быть приписан к его изобретениям, так как он является типовым. Важно отметить, что при отправке своих сообщений в Москву Зорге предпочитал использовать английский язык. В качестве основы для построения шахматного шифра применялось слово SUBWAY, которое записывалось в первой строке квадратной матрицы. Затем в оставшиеся ячейки матрицы по порядку вписывались буквы английского алфавита, которые не входили в ключевое слово. Таким образом, для ключа SUBWAY будет получена следующая матрица:

Таблица 29. Матрица с ключевым словом

S	U	B	W	A	Y
C	D	E	F	G	H
I	J	K	L	M	N
O	P	Q	R	T	V
X	Z	.	/		

Точка и слеш используются для разделения слов или для обозначения перехода на цифровой текст. На втором этапе построения шифра использовалась анаграмма ASINTOER, которая состояла из наиболее часто встречающихся символов. Буквы, входящие в анаграмму, нумеруются по порядку по столбцам (табл. 30), и далее эти символы составляют первую строку новой таблицы. Остальные строки заполняются по остаточному принципу (табл. 31) и обозначаются с помощью двоичных чисел в диапазоне от 80 до 99.

Таблица 30. Таблица с вероятностями

S=0	U	B	W	A=5	Y
C	D	E=3	F	G	H
I=1	J	K	L	M	N=7
O=2	P	Q	R=4	T=6	V
X	Z	.	/		

Таблица 31. Заполнение матрицы по остаточному принципу

	0	1	2	3	4	5	6	7	8	9
-	S	I	O	E	R	A	T	N	-	-
8	C	X	U	D	J	P	Z	B	K	Q
9	.	W	F	L	/	G	M	Y	H	V

Таблица 32. Пример шифрования

Исходное сообщение	PRACTICE MAKES PERFECT
Ключ	Шифр Рамзая таблица х.х
Зашифрованное сообщение	85458 06180 39496 58830 94853 49238 06

Пояснение: P→85, R→4, A→5, C→80, T→6, I→1, C→80, E→3, /→94, M→96, A→5, K→88, E→3, S→0, /→94, P→85, E→3, R→4, F→92, E→3, C→80, T→6

Полученная последовательность разбивается на пятизначные группы:

85458 06180 39496 58830 94853 49238 06

Задача: Имея исходное/зашифрованное сообщение и ключ, получить зашифрованное/исходное сообщение.

Вариант 1

Зашифровать

Исходное сообщение	MY NAME IS (ВАШЕ ИМЯ)
--------------------	-----------------------

Вариант 2

Расшифровать

Зашифрованное сообщение	73993 49495 19939 48285
-------------------------	-------------------------

Вариант 3

Зашифровать

Исходное сообщение	I LIVE IN MOSCOW
--------------------	------------------

Вариант 4

Расшифровать

Зашифрованное сообщение	93278 32794 10946 98394 80585 16593 94292 94958 7
-------------------------	--

Вариант 5

Зашифровать

Исходное сообщение	I STUDY AT RTU MIREA
--------------------	----------------------

Вариант 6

Зашифровать

Исходное сообщение	TO DO SOMEONE A FAVOUR
--------------------	------------------------

Вариант 7

Зашифровать

Исходное сообщение	TO BREAK THE NEWS TO SOMEONE
--------------------	---------------------------------

Вариант 8

Зашифровать

Исходное сообщение	THE FORBIDDEN FRUIT IS ALWAYS THE SWEETEST
--------------------	---

Вариант 9

Зашифровать

Исходное сообщение	TO SAVE A SEAT FOR SOMEONE
--------------------	----------------------------

Вариант 10

Зашифровать

Исходное сообщение	TOO MANY COOKS SPOIL THE BROTH
--------------------	-----------------------------------

Шифр Рубика

Для шифрования фразы был взят кубик Рубика 2x2. Развёртка кубика показана на рис. 20.

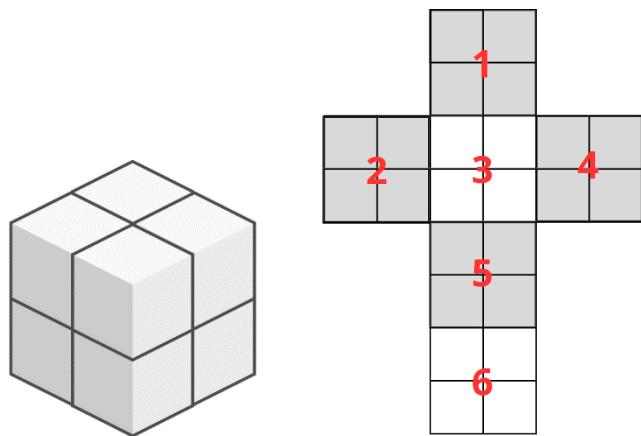


Рисунок 20. Кубик 2х2 и развертка

Для шифрования будет использоваться исходное сообщение: РТУ МИРЭА.

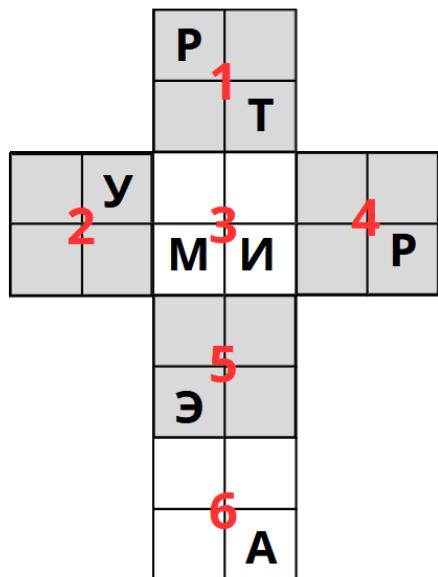


Рисунок 21. Нанесённые буквы на развертку кубика

Для шифрования будут использованы следующие повороты:
Грань №1 вправо 1 раз (рис. 22).

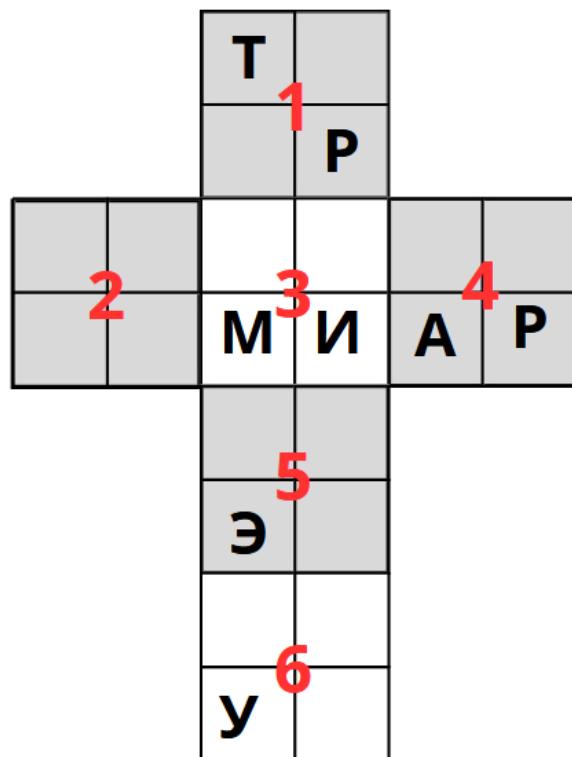


Рисунок 22. Поворот 1 грани вправо

Грань №3 вправо 1 раз (рис. 23).

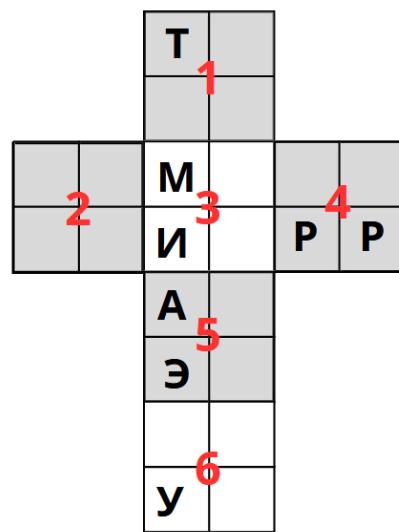


Рисунок 23. Поворот 3 грани право

Грань №4; вправо 2 раза (рис. 24).

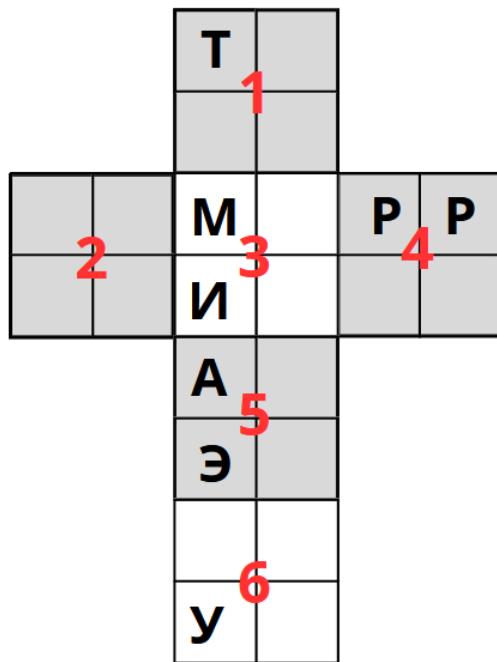


Рисунок 24. Поворот 4 грани вправо

Таким образом, зашифрованное сообщение: ТМРРИАЭУ.

Задача: Имея зашифрованное сообщение и исходные ключи (как были повернуты грани для шифрования), получить исходное сообщение/Зашифровать исходное сообщение, если известно расположение букв и ключ(поворот граней).

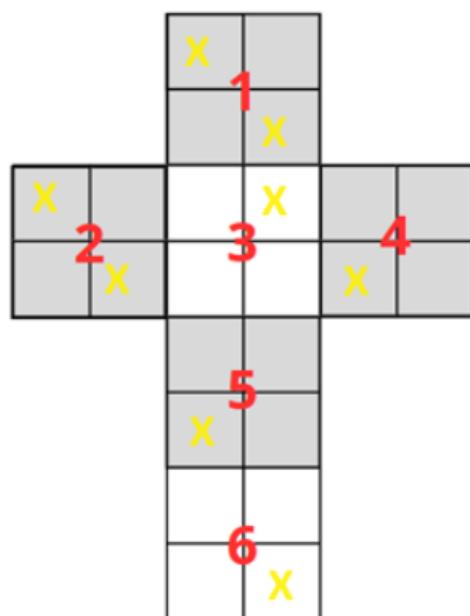
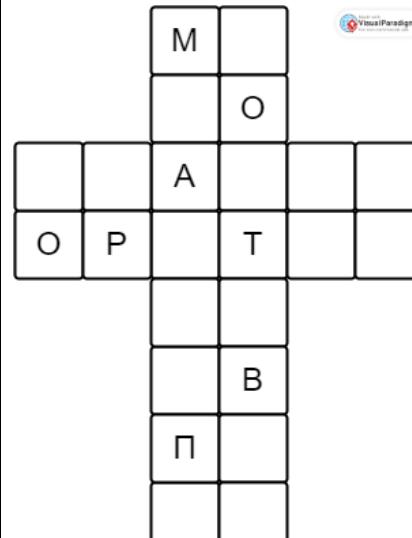
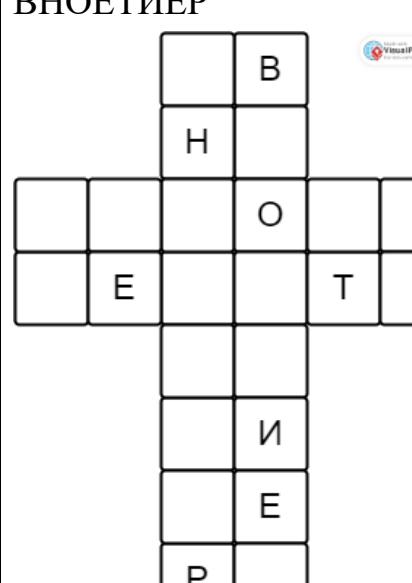


Рисунок 25. Расположение букв для шифрования

Вариант 1

Ключ	Грань №2 вправо 1 раз Грань №4 влево 2 раза Грань №5 вправо 1 раз
Зашифрованное сообщение	<p>МОАОРТВП</p> 

Вариант 2

Ключ	Грань №5 влево 2 раза Грань №1 вправо 1 раз Грань №3 вправо 1 раз
Зашифрованное сообщение	<p>ВНОЕТИЕР</p> 

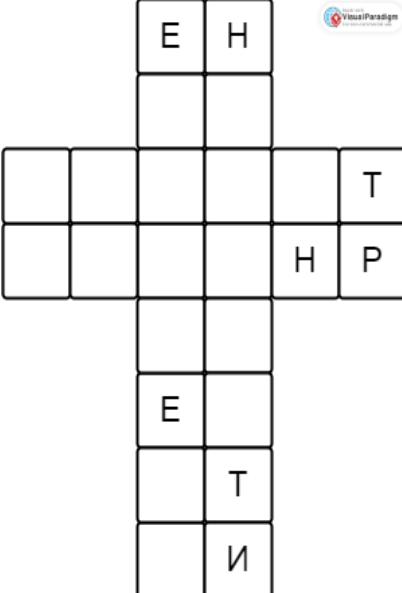
Вариант 3

Ключ	Грань №2 влево 1 раз Грань №5 вправо 2 раза Грань №1 вправо раз
Зашифрованное сообщение	<p>БРОИНООД</p>

Вариант 4

Ключ	Грань №4 вправо 3 раза Грань №1 вправо 1 раз Грань №5 влево 1 раз
Зашифрованное сообщение	<p>ДРНИОВАЗ</p>

Вариант 5

Ключ	Грань №3 влево 1 раз Грань №2 вправо 2 раза Грань №1 влево 1 раз
Зашифрованное сообщение	<p>ЕНТНРЕТИ</p> 

Вариант 6

Исходное сообщение	авангард
Ключ	Грань №3 влево 1 раз Грань №2 вправо 2 раза Грань №1 влево 1 раз

Вариант 7

Исходное сообщение	взаимный
Ключ	Грань №3 влево 1 раз Грань №2 вправо 2 раза Грань №1 влево 1 раз

Вариант 8

Исходное сообщение	душистый
Ключ	Грань №3 влево 1 раз Грань №2 вправо 2 раза Грань №1 влево 1 раз

Вариант 9

Исходное сообщение	здоровый
Ключ	Грань №3 влево 1 раз Грань №2 вправо 2 раза Грань №1 влево 1 раз

Вариант 10

Исходное сообщение	ласковый
Ключ	Грань №3 влево 1 раз Грань №2 вправо 2 раза Грань №1 влево 1 раз